

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-143621

(43)Date of publication of application : 29.05.1998

(51)Int.CI.

G06K 17/00  
G03H 1/22  
G06F 17/60  
G06F 19/00  
G06K 19/10  
G06K 19/06

(21)Application number : 08-286490

(71)Applicant : AMERICAN BANK NOTE HOLOGRAPHIC INC

(22)Date of filing : 29.10.1996

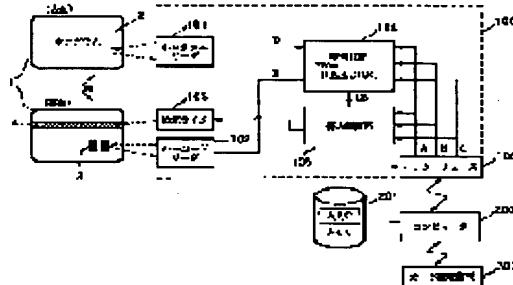
(72)Inventor : LILLEY OBOIRU  
DAA KUAN KAN

(54) CARD SECURITY SYSTEM, METHOD FOR IMPROVING SECURITY, CARD READING DEVICE AND CARD ISSUING DEVICE AND HOLOGRAM READING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To efficiently improve security in a card security system using an identification card or the like.

SOLUTION: In a card security system equipped with a card issuing device 100 and a card reading device 300, the card issuing device 100 reads a hologram 2 and a bar code 3 on a card 1, and obtains data D and E. Also, data A, B, and C are inputted from a computer 200 to the card issuing device 100. An enciphering part 104 generates check data EN based on the data A-E, and a magnetic writer 103 writes the data A-C and EN in a magnetic stripe 4. The card reading device 300 reads the data A-E from the card 1, calculates check data by using this, and compares the check data with the check data EN recorded in the magnetic strip 4 for judging the authenticity of the card.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51) Int.Cl.<sup>6</sup>  
 G 0 6 K 17/00  
 G 0 3 H 1/22  
 G 0 6 F 17/60  
 19/00  
 G 0 6 K 19/10

識別記号

F I  
 G 0 6 K 17/00 T  
 G 0 3 H 1/22  
 G 0 6 F 15/21 3 4 0 C  
 15/30 3 5 0 Z  
 G 0 6 K 19/00 R

審査請求 未請求 請求項の数21 OL (全 15 頁) 最終頁に続く

(21)出願番号 特願平8-286490

(22)出願日 平成8年(1996)10月29日

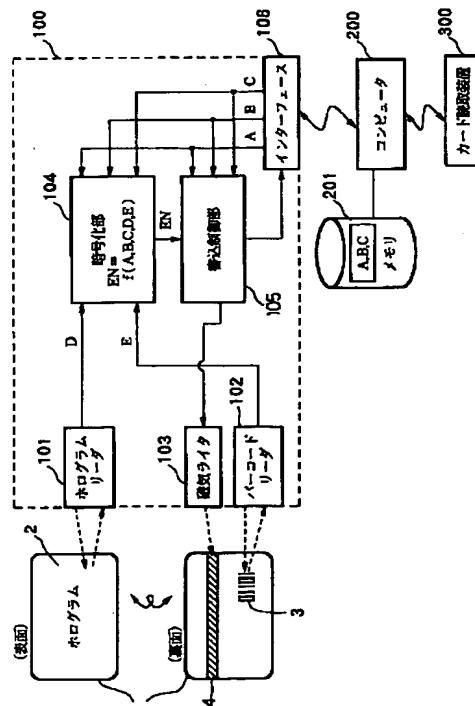
(71)出願人 594074779  
 アメリカン パンク ノート ホログラフ  
 イクス, インク.  
 アメリカ合衆国 10523 ニューヨーク、  
 エルムスフォード イグゼキュティブ ブ  
 ルバード 399  
 (72)発明者 リリイ オボイール  
 アメリカ合衆国 ニューヨーク州 コート  
 ランド マナー (番地無し)  
 (72)発明者 ダー・クアン カン  
 アメリカ合衆国 ニューヨーク州 クロー  
 トン オン ハドソン (番地無し)  
 (74)代理人 弁理士 大塚 康徳 (外1名)

(54)【発明の名称】 カードセキュリティシステム及びセキュリティ向上方法及びカード読取装置及びカード発行装置  
 及びホログラム読取装置

## (57)【要約】

【課題】識別カード等を用いたカードセキュリティシステムにおけるセキュリティを効果的に向上する。

【解決手段】カード発行装置100とカード読取装置300を備えるカードセキュリティシステムにおいて、カード発行装置100はカード1上のホログラム2及びバーコード3を読み取りデータD、Eを得る。また、コンピュータ200よりカード発行装置100にデータA、B、Cが入力される。暗号化部104は、データA～Eに基づいてチェックデータENを生成し、磁気ライタ103はデータA～C及びENを磁気ストライプ4に書込む。カード読取装置300では、カード1よりデータA～Eを読み取り、これらを用いてチェックデータを算出し、磁気ストライプ4に記録されたチェックデータENと比較することでカードの真正を判断する。



## 【特許請求の範囲】

【請求項 1】 カード発行装置とカード読取装置を備えるカードセキュリティシステムにおけるセキュリティの向上方法であって、

カード上の光学的読取部分に少なくとも第 1 のデータを記録する第 1 記録工程と、

前記カード発行装置に少なくとも第 2 のデータを入力する入力工程と、

少なくとも前記第 1 のデータと前記第 2 のデータに基づいてチェックデータを獲得する獲得工程と、

少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する第 2 記録工程と、

少なくとも前記光学的読取部分を読み取って得られるデータと、前記格納媒体より得られるデータと、前記入力工程で用いられた前記第 2 のデータに基づいて、前記カード読取装置によりカードの正当性を検証する検証工程とを備えることを特徴とするセキュリティの向上方法。

【請求項 2】 前記格納媒体は、前記カード上の磁気的読取部分あるいは光学的読取部分、前記カードに搭載されたメモリ、あるいは該カードとは別体のメモリの少なくとも 1 つで構成されることを特徴とする請求項 1 に記載のセキュリティの向上方法。

【請求項 3】 前記第 2 記録工程は、前記チェックデータ及び前記第 2 のデータを前記格納媒体に記録し、前記検証工程は、前記チェックデータ及び前記第 2 のデータとしてのデータを前記格納媒体より得ることを特徴とする請求項 1 に記載のセキュリティの向上方法。

【請求項 4】 前記格納媒体は、前記カード上の磁気的読取部分及び前記カードとは別体のメモリを含み、前記第 2 記録工程は、全チェックデータ及び前記第 2 のデータを前記磁気的読取部分と前記メモリに分けて記録することを特徴とする請求項 3 に記載のセキュリティの向上方法。

【請求項 5】 前記第 1 記録工程は前記第 1 のデータをホログラフィックイメージにて記録することを特徴とする請求項 1 に記載のセキュリティの向上方法。

【請求項 6】 前記獲得工程は、少なくとも前記第 1 のデータと前記第 2 のデータを暗号化することにより前記チェックデータを決定することを特徴とする請求項 1 に記載のセキュリティの向上方法。

【請求項 7】 カード発行装置とカード読取装置を備えるカードセキュリティシステムであって、

カード上の光学的読取部分より少なくとも第 1 のデータを読み取る読取手段と、

前記カード発行装置に少なくとも第 2 のデータを入力する入力手段と、

少なくとも前記第 1 のデータと前記第 2 のデータに基づいてチェックデータを獲得する獲得手段と、

少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する記録手段と、

少なくとも前記光学的読取部分を読み取って得られる第 1 のデータと、前記格納媒体より得られるチェックデータと、前記入力手段で用いた前記第 2 のデータとに基づいて、前記カード読取装置によりカードの正当性を検証する検証手段とを備えることを特徴とするカードセキュリティシステム。

【請求項 8】 光学的読取部分を含むカードの読み取りを行うためのカード読取装置であって、

少なくとも第 1 のデータを前記光学的読取部分より読み取る光学読取手段と、

少なくとも第 2 のデータ及び第 3 のデータを格納媒体より獲得する第 1 獲得手段と、

少なくとも前記第 1 のデータおよび前記第 2 のデータに基づいてチェックデータを算出する第 2 獲得手段と、

前記第 1 獲得手段で獲得した第 3 のデータと前記第 2 獲得手段で獲得したチェックデータとを比較し、当該カードが正当か否かを判定する判定手段とを備えることを特徴とするカード読取装置。

【請求項 9】 前記格納媒体は、前記カード上に設けられた磁気的読取部分、光学的読取部分、該カードに搭載されたメモリ、あるいは該カードとは別体のメモリユニットの少なくとも 1 つによって構成されることを特徴とする請求項 8 に記載のカード読取装置。

【請求項 10】 前記第 1 獲得手段は、前記第 2 のデータを前記メモリユニットより獲得し、前記第 3 のデータを前記磁気的読取部分より獲得することを特徴とする請求項 9 に記載のカード読取装置。

【請求項 11】 前記格納媒体は前記カード上の磁気ストライプを含み、

当該カードの使用後に前記磁気ストライプ上のデータを無効化する無効化手段を更に備えることを特徴とする請求項 8 に記載のカード読取装置。

【請求項 12】 カードの発行を行うカード発行装置であって、

光学的読取部分より少なくとも第 1 のデータを読み取る読取手段と、

カードとは別体の記憶部より少なくとも第 2 のデータを入力する入力手段と、

少なくとも前記第 1 のデータおよび前記第 2 のデータに基づいてチェックデータを決定する決定手段と、

少なくとも前記決定されたチェックデータを格納媒体に記録する記録手段とを備えることを特徴とするカード発行装置。

【請求項 13】 前記格納媒体は、前記カード上に設けられた磁気的読取部分、光学的読取部分、該カードに搭載されたメモリあるいは該カードとは別体のメモリユニットの少なくとも 1 つによって構成されることを特徴と

する請求項12に記載のカード発行装置。

【請求項14】前記記録手段は、前記チェックデータを当該カード上の磁気的読取部分に記録し、前記第2のデータを前記メモリユニットに記録することを特徴とする請求項13に記載のカード発行装置。

【請求項15】ホログラムイメージ上に所定の方向から光を照射する照射手段と、

前記照射手段で照射された光の前記ホログラムイメージからの反射光によって空間に形成される再生像の光強度分布を検出する検出手段と、

前記検出手段で検出された光強度分布を出力する出力手段とを備えることを特徴とするホログラム読取装置。

【請求項16】前記再生像の相対的な光強度に基づいて前記検出手段によって検出された前記光強度分布を2値化する2値化手段を更に備え、

前記出力手段は前記2値化手段で得られる2値化データを出力することを特徴とする請求項15に記載のホログラム読取装置。

【請求項17】異なるパターン像を形成するべく前記再生像を処理する処理手段を更に備え、

前記検出手段は、前記パターン像の光強度分布を検出することを特徴とする請求項15に記載のホログラム読取装置。

【請求項18】前記処理手段は、所定のパターン像を前記再生像に干渉させることで該再生像を処理することを特徴とする請求項17に記載のホログラム読取装置。

【請求項19】前記検出手段で検出された光強度分布に対応するパターンデータをデジタル的に処理し、別のパターンデータを形成する処理手段を更に備え、

前記出力手段は前記処理手段で形成された前記別のパターンを出力することを特徴とする請求項15に記載のホログラム読取装置。

【請求項20】ホログラムイメージ上に所定の方向から光を照射する照射手段と、

前記照射手段で照射された光の前記ホログラムイメージからの反射光に所定の光波を干渉させ、パターンイメージを形成する干渉手段と、

前記干渉手段で形成されたパターンイメージの光強度分布を検出する検出手段と、

前記検出手段で検出された光強度分布を出力する出力手段とを備えることを特徴とするホログラム読取装置。

【請求項21】前記ホログラムイメージはフーリエ変換パターンであることを特徴とする請求項15乃至20のいずれかに記載のホログラム読取装置。

#### 【発明の詳細な説明】

##### 【0001】

【産業上の利用分野】本発明は、クレジットカード、IDカード、運転免許証等の如き識別カードを利用したカードセキュリティシステム及びセキュリティ向上方法及びカード読取装置及びカード発行装置及び該カードセキ

ュリティシステムに好適なホログラム読取装置に関する。

##### 【0002】

【従来の技術】クレジットカードが発行された初期の時代は、銀行がカードを見境なく発行し、ブランクカードに対する管理は手ぬるかった。すなわち、多くのカードに銀行名を入れただけのブランクのクレジットカードが存在し、これらが犯罪者に利用されていた。さらに、カードの信頼性を保つための印刷手法も欠如していたので、犯罪者は容易に真正カードに代わる偽造カードをつくることができ、このような犯罪が多発していた。

【0003】銀行側の損失がエスカレートするにつれて、銀行はカードの発行を許可する顧客を厳しく制限するとともに、カード自体のデザインや製造上のセキュリティを向上する手段を講ずるようになった。多くの手段が考えられるが、犯罪者にとっての主たるカード資源、すなわち、偽造カードを事実上なくしたのは、ホログラフィーによって生成した回折格子を有する一枚の箔をカードの前面に導入することであった。しかし、それでも犯罪者には、次の3つの理由に基づく詐欺行為の道が残されていたのである。

【0004】第1は、盗難もしくは遺失カードで、カード所有者からの報告が届くまでの間に、これを使用することである。第2は、旧式もしくは遺失カードではあるが、かつて有効なカードであったものに有効な口座番号を再コード化して使用することである。第3は有効番号を使用する（カード無しに）こと、もしくはATMで使用するための磁気ストライプを有する白カードを使用すること、或いは、人による認証ではなく機械読みのみによる認証が行われる電話を使用することである。實際には、カード自体が正当なものであると断言しようとする第4のタイプの詐欺行為もある。マスターカードとビザがこの分野においてホログラムを8年間用いてきた。しかし、間もなく、何者かが、何処かで、受容され得る偽造カードを製造するのに十分な技術を獲得するようになるであろう。よって、犯罪者の偽造行為に一步先んじた防衛手段のための安全印刷の時機が再び到来したと考えるべきである。

##### 【0005】

【発明が解決しようとする課題】今日の技術では第1の盗難もしくは遺失タイプの詐欺行為については防衛手段は殆どない。しかしながら、本発明は、第2、第3、第4のタイプの犯罪行為に対しては安全性を有効に増進することができる。

【0006】典型的なクレジットカード取引は販売員がカードを見て、有効と思えば、カードを磁気リーダに打ち込む。これはChang et alの米国特許第4,788,420号に開示された方法である。リーダは取引口座アクセス識別番号を認証元に送り戻す。そして、認証元から許諾の応答があれば取引が実行される。結局、合法的なカード

の所有者が計算書を受け取り、当該所有者はこの計算書に対して支払いもしくは否認をすることになる。もし、カードの所有者によって正当に否認されると、磁気リーダは手続上認可された取引口座アクセス識別番号を提供したのであるから、結局は銀行が損失を吸収しなければならないであろう。これが第1及び第2のタイプの詐欺において発生するのである。

【0007】磁気ストライプに書き込まれたりコード化された取引口座アクセス識別番号は車のナンバープレートに非常によく似ている。ナンバープレートには沢山の情報はないし、磁気ストライプにも沢山の情報がない。支払いの歴史、顧客の母親の旧姓等、真に価値ある情報は、すべて銀行の情報システムの奥に貯蔵される。そのクレジットが有効かどうかのみが、販売現場からの要求によって到達する。

【0008】上記の状況は自動車のプレートないしは登録ナンバーに似ている。すなわち、情報はあまり沢山ではなく、丁度、自動車省のファイルに貯蔵されている情報に到達する手法である。

【0009】顧客側の少量の銀行情報（カードの有効期間、有効なクレジット量）へのアクセスは、取引を読み取り報告するのに利用できる装置によってクレジットカードが打ち込まれ或いは磁気的に読み取られた際に、電子ネットワークを介して隨時商人に利用可能である。

【0010】不法な目的のための一般に受容され得るクレジットカードの供給は不完全かつ少量であるが、物理的には真正であるが旧式になってしまったクレジットカードを取得して磁気情報を変えたり、カード上面の満了期日や氏名を再エンボス加工することは、犯罪者には依然として比較的容易である。元の氏名を消して再エンボスしたものは完全ではないのにもかかわらず、このような詐欺に慣れた人の周到な準備によって、この世俗的な詐欺手段は一般には成功する。そこで、カードを打って、クレジット相当の勘定が識別され、マシンには取引有効の緑信号が出る。

【0011】とくにATMのような場合では、犯罪者が唯一必要とすることは、磁気的に読み取れる取引口座アクセス識別番号と、何も知らない被害者の個人識別番号

（PIN）とをコード化した磁気テープを有する白カードである。また、電話室とか、スーパーマーケットのような、個人識別番号が不要であり、事務員による実カードの照合がなされないような場所も沢山ある。

【0012】磁気エンコードのセキュリティを高めたり、書換を妨げるような試みが長期に亘って積極的に試みられた。Thorne-EMIのWatermark（商標）テープがその一例であった。3M社等の高エルステッドテープの開発も同じ例である。両者とも、幾らか限定されたものではあるが、セキュリティの向上をそれぞれの方針において提供した。しかし、両者とも、現在使われている処理を変更しなければならないため、業界には受容されな

かった。

【0013】Thorne-EMIの方法はテープが製造されている間にテープに連続番号を磁気的に組み込んでしまうという方法である。これは磁気リーダで読み取りができる。しかし、この方法はテープ製造の困難さや、連続番号であることもあって挫折した。このような方法はコストが掛かり過ぎると考えられている。

【0014】3M社の方法は300エルステッドテープ（業界の標準）をコード化するのに使用されるものよりも、もっと強力なコード化装置が必要な高い飽和保磁力を有するテープの製造ということであった。このような装置は容易には得られないので、安全性が辛うじて増進された。業界はさらに強い飽和保磁力テープを指向した。しかしサービス業も銀行もこれにあわせて新しいエンコード装置を買い求めなければならなかった。これは、そうすることに確固たる動機を持ち合わせないグループにとっては大きな設備投資であり、このような高い飽和保磁力テープのエンコード装置が犯罪者には利用されないのであるという見通しもなかった。以上のような状態で、強力なテープも装置も、僅かな変化しか期待することができなかった。

【0015】磁気的な読取環境に記録されたものはどんなものであっても、磁気エンコードを読み取る初步的な装置によって誰でも読み取ることができる。コード化され、或いは暗号化されることによって数字が意味をなさなくとも、そのコード化された、或いは暗号化された数字を模写することは依然として容易である。過去に欠如していたものは、即ち本発明が解決しようとするものであるが、従来の装置では読み取ることのできないもう一つのレベルの、費用効果の良い方法で磁気ストライプに書き込みが可能な数字である。

【0016】磁気番号のアルゴリズムを含むすべての他のいかなる努力も、それがどんなに入り組んだ複雑なものであっても弱点を有している。その理由は、オリジナルであっても偽造したものであっても、全ての磁気番号を磁気リーダで読み取ることができ、読み取った番号を検証のために、通信網に乗せて銀行に送ることができるからである。

【0017】問題解決の方法として、カード製造会社が大部分のクレジットカードにバッチナンバーを印刷している。全てのアメリカンエキスプレスのカードや幾つかのマスターカードに見られる4桁数字が一般的である。取引が詐欺らしいという疑いがある時は、カードの有効性について発行銀行に電話をして、a) バッチ番号は真正であって盗用されたものではないか、b) カードの上の個人に係属する磁気情報がカードの前面のバッチ番号に合致するかどうか、を調べるのである。

【0018】この方法は、カードを差し出した相手が取引に相応しくない風体であった場合、例えば汚いスニーカーを履いた十代の若者が真新しい自動車を買おうとす

る場合とか、なにか落ち着かない状況にある場合にのみ詐欺だと決める不完全かつ努力を必要とする方法である。

【0019】1989年8月8日発行のTomiyama et alの米国特許第4,855,584号には別の方法が開示されている。これはカードを機械で2回読みすることで、データを電話連絡する必要をなくすものである。しかしながら、この方法では実際には磁気ストライプのように作用するバーコードを使うことによって証明媒体を隠してしまう必要がある。この実施できそうもないのみならず、磁気リーダにバーコード（磁気インクで印刷されている）を読みませ、そしてそのバーコードがIRリーダでのみ見られるように印刷されてあつたとしても、詐欺師は下にある情報を、それが磁気的読取媒体であるため解読できる。

【0020】全ての犯罪者が必要とすることは番号全体をコピーすることである。問題は、カラーゼロックス機でコピーすることができない視覚安全形態或いはシステムを創造しようとする試みに似ている。人間の視力が安全の形態を見ることができる限りはカラーコピー機もそれができる。すべての試みはコピー機を打ち負かすためになってきたが、これを書いている時点ではすべての（極端に厄介な又は非実用的な）ものは失敗した。クレジットカードの確認という問題は、新規性があり非常に実際的な解決である。

【0021】本発明は上述した問題に鑑みてなされたものであり、カード等のセキュリティを効果的に向上するカードセキュリティシステム及びそのセキュリティ向上方法及び該システムにおけるカード読取装置及びカード発行装置及び該カード読取装置に適用可能なホログラム読取装置を提供することを目的とする。

【0022】

【課題を解決するための手段】上記の目的を達成するための本発明のカードセキュリティシステムにおけるセキュリティ向上方法は以下の工程を備える。すなわち、カード発行装置とカード読取装置を備えるカードセキュリティシステムにおけるセキュリティの向上方法であつて、カード上の光学的読取部分に少なくとも第1のデータを記録する第1記録工程と、前記カード発行装置に少なくとも第2のデータを入力する入力工程と、少なくとも前記第1のデータと前記第2のデータに基づいてチェックデータを獲得する獲得工程と、少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する第2記録工程と、少なくとも前記光学的読取部分を読み取って得られるデータと、前記格納媒体より得られるデータと、前記入力工程で用いられた前記第2のデータとに基づいて前記カード読取装置によりカードの正当性を検証する検証工程とを備える。

【0023】また、上記の目的を達成するための本発明

のカードセキュリティシステムは以下の構成を備える。すなわち、カード発行装置とカード読取装置を備えるカードセキュリティシステムであつて、カード上の光学的読取部分より少なくとも第1のデータを読み取る読取手段と、前記カード発行装置に少なくとも第2のデータを入力する入力手段と、少なくとも前記第1のデータと前記第2のデータに基づいてチェックデータを獲得する獲得手段と、少なくとも前記チェックデータを、少なくとも前記カード読取装置からアクセス可能な格納媒体に記録する記録手段と、少なくとも前記光学的読取部分を読み取って得られる第1のデータと、前記格納媒体より得られるチェックデータと、前記入力手段で用いた前記第2のデータとに基づいて、前記カード読取装置によりカードの正当性を検証する検証手段とを備える。

【0024】また、上記の目的を達成するための本発明のカード読取装置は、光学的読取部分を含むカードの読み取りを行うためのカード読取装置であつて、少なくとも第1のデータを前記光学的読取部分より読み取る光学読取手段と、少なくとも第2のデータ及び第3のデータを格納媒体より獲得する第1獲得手段と、少なくとも前記第1のデータおよび前記第2のデータに基づいてチェックデータを算出する第2獲得手段と、前記第1獲得手段で獲得した第3のデータと前記第2獲得手段で獲得したチェックデータとを比較し、当該カードが正当か否かを判定する判定手段とを備える。

【0025】また、上記目的を達成するための本発明のカード発行装置は以下の構成を備える。すなわち、カードの発行を行うカード発行装置であつて、光学的読取部分より少なくとも第1のデータを読み取る読取手段と、カードとは別体の記憶部より少なくとも第2のデータを入力する入力手段と、少なくとも前記第1のデータおよび前記第2のデータに基づいてチェックデータを決定する決定手段と、少なくとも前記決定されたチェックデータを格納媒体に記録する記録手段とを備える。

【0026】更に、上記の目的を達成する本発明のホログラム読取装置は、ホログラムイメージ上に所定の方向から光を照射する照射手段と、前記照射手段で照射された光の前記ホログラムイメージからの反射光によって空間に形成される再生像の光強度分布を検出する検出手段と、前記検出手段で検出された光強度分布を出力する出力手段とを備える。

【0027】更に、上記の目的を達成する本発明の他の構成によるホログラム読取装置は以下の構成を備える。すなわち、ホログラムイメージ上に所定の方向から光を照射する照射手段と、前記照射手段で照射された光の前記ホログラムイメージからの反射光に所定の光波を干渉させ、パターンイメージを形成する干渉手段と、前記干渉手段で形成されたパターンイメージの光強度分布を検出する検出手段と、前記検出手段で検出された光強度分布を出力する出力手段とを備える。

【0028】なお、本発明において、カードとはいわゆるクレジットカードやIDカード等種々のカードを総称するものである。更に、本発明におけるカードは、銀行通帳のようなセキュリティを要する帳面、文書等をも含むものである。

【0029】

【発明の実施の形態】以下、添付の図面を参照して本発明の好適な一実施形態を説明する。

【0030】図1は、本実施形態のカードセキュリティシステムに用いられる識別カードの概観を示す図である。1は識別カードであり、その前面にはホログラムイメージ2が記録されている。そして、このホログラムイメージ2の全体あるいは一部分には、第1の光学的記録部分としてのホログラムコードが記録されている。また、識別カード1の裏面には、第2の光学的記録部分としてのバーコード3が印刷されている。更に識別カード1の裏面には、磁気ストライプ4が設けられている。なお、バーコード3としては、1次元バーコードが図示されているが、2次元バーコードを用いてもよい。

【0031】図2は本実施形態のカードセキュリティシステムにおけるカード発行装置の構成を示すブロック図である。同図において、識別カード1は上述のごとく、その表面にはホログラムイメージ2を、裏面には磁気ストライプ4、バーコード3を有する。図1では、ホログラムイメージは識別カード1の表面の全体に記録されているが、カード表面の一部に記録されていてもよい。また、ホログラムコードの記録も、ホログラムイメージの一部もしくは全てとして記録される。ホログラムコードとしては、例えば3次元バーコードイメージが記録されており、後述のホログラムリーダ101によって読み取り可能である。

【0032】100は本実施形態のカード発行装置であり、カード発行装置100は以下のように構成されている。101はホログラムリーダであり、識別カード1に記録されたホログラムに所定特性の光をあて、ホログラムイメージ2よりの反射光によって再生される再生像

(3次元バーコードイメージ)から、当該ホログラムイメージ2に記録されているデータを読み取る。102は周知のバーコードリーダであり、本例では1次元バーコードであるバーコード3を読み取ってデータを得る。103は磁気ライタであり、磁気ストライプ4にデータを記録する。なお、ホログラムリーダ101が3次元バーコードイメージを走査して得た信号はディジタルデータに変換され、データDとして出力される。また、バーコードリーダ102がバーコード3を走査して得た信号は、ディジタルデータに変換され、データEとして出力される。

【0033】104は暗号化部であり、ホログラムリーダ101がホログラムイメージ2を読み取って得たデータDと、バーコードリーダ102がバーコード3を読み

取って得たデータEと、外部装置であるコンピュータ200よりインターフェース106を介して得たデータA、B、Cを用いて所定の演算を行い、チェックデータENを発生する (EN = f (A, B, C, D, E) とする)。105は書込制御部であり、暗号化部104より得られたチェックデータENを磁気ライタ103を介して磁気ストライプ4に書込む。更に、書込制御部105は、インターフェース106を介して入力されたデータA、B、Cを、磁気ライタ103を介して磁気ストライプ4に書込む。

【0034】106はインターフェースであり、外部のコンピュータ200と当該カード発行装置100の間の通信を行う。コンピュータ200はカード発行装置100に接続されると共に、カード読取装置300にも接続されており、この結果メモリ201はカード発行装置100及びカード読取装置300の何れからもアクセス可能である。なお、カード読取装置300の詳細な構成については後述する。メモリ201にはデータA、B、Cが格納されており、カード発行装置100からの要求を受けたコンピュータ200がこれらのデータをカード発行装置100に出力する。

【0035】ここで、例えば、データDとしては、当該カードの価値を示す金額データであり、データEとしては当該カードの固有の番号を示す識別番号(ID)である。また、インターフェース106を介して入力されるコンピュータ200よりのデータA、B、Cとしては、例えば、それぞれ日付、店番号、パスワードを示すデータである。以下の説明では、これらのデータが識別カード1に記録されるものとして説明する。

【0036】なお、上述した磁気ストライプ4へ書込まれるデータA、B、C及びチェックデータENの内の一  
部もしくはすべてをコンピュータ200に接続されたメモリ201に格納しておくように構成することができるが、この点は本実施形態の変形例において詳細に説明する。

【0037】図3は本実施形態におけるカード読取装置の構成を示すブロック図である。ホログラムリーダ301は、処理対象である識別カード1に記録されたホログラムイメージ2上のホログラムコードを読み取り、これを当該カードの金額を示すデータDrとして暗号化部304へ出力する。バーコードリーダ302は、バーコード3を読み取り、これを当該カードの識別番号を示すデータErとして暗号化部304へ出力する。磁気リーダ303は、磁気ストライプ4に記録されている、日付、店番号、パスワードを読み取り、データAr、Br、Crとして暗号化部304へ出力する。更に、磁気リーダ303は、磁気ストライプ4に記録されているチェックデータを読み取り、これをチェックデータENrとして判定部306へ出力する。

【0038】304は暗号化部であり、入力されたデータ

タA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>、D<sub>r</sub>、E<sub>r</sub>に基づいてチェックデータE<sub>Nr'</sub>を算出する。ここで、暗号化部304におけるチェックデータの算出アルゴリズム（暗号化演算）は暗号化部104（図2）のそれと同じである。305はインターフェースであり、コンピュータ200とカード読取装置300との間の通信を制御する。本実施形態のインターフェースは、ホログラムリーダ301、バーコードリーダ302、磁気リーダ303から得られるデータA<sub>r</sub>～E<sub>r</sub>をコンピュータ200に対して送信する。コンピュータ200は、カード読取装置300より受信したデータA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>とメモリ201に格納されているデータA、B、Cとを比較して、データA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>の正当性を検証する。そして、インターフェース305は、データの正当性を検証した結果をコンピュータ200より受信する。この受信された正当性の検証結果は、判定部306へ入力される。

【0039】なお、カード発行装置100による識別カード1の発行時に、コンピュータ200が発行対象の識別カードのID番号を入力し、ID番号とデータA、B、Cとを対応付けるテーブルをメモリ201に格納しておくようにしてもよい。この場合、カードの正当性の検証に際しては、カード読取装置300より入力したID番号（データE<sub>r</sub>）に基づいてテーブルを検索し、対応するデータA、B、Cを抽出する。そして、カード読取装置より入力したデータA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>のそれぞれと比較することで、データの正当性をチェックするようになる。こうすれば、A、B、Cをカード毎に設定することができる。例えば、カード毎にパスワードを変更することが可能となる。

【0040】判定部306は、磁気リーダ303が磁気ストライプ4より読み取ったチェックデータE<sub>Nr</sub>と、暗号化部304で得られたチェックデータE<sub>Nr'</sub>とを比較する。判定部306は、この比較の結果両者が一致し、更にインターフェース305より入力された検証結果が正当であることを示している場合に、当該カードを受理し、処理部307に所定の処理の実行を指示する。本例では、読み取られた識別カード1のホログラムイメージ2として記録された金額データ（データD<sub>r</sub>）に基づいて、現金の支払いを行うものとする。

【0041】以上の構成を備えた本実施形態のカード発行装置100、カード読取装置300の動作をフローチャートを参照して説明する。

【0042】図4は、第1の実施形態によるカード発行装置100の動作手順を説明するフローチャートである。本例では、ホログラムコード（金額データ）を含むホログラムイメージとID番号を示す1次元バーコードとが記録されたカードをカード発行装置100に供給しておき、磁気ストライプに所定のデータ書込が行われた識別カードが発行されるものとする。

【0043】ステップS11において、ホログラムリー

ダ301を用いて、供給された識別カード1のホログラムイメージ2を読み取り、データD（金額データ）を得る。また、ステップS12において、バーコードリーダ302により識別カード1上のバーコード3を読み取り、データE（ID番号）を得る。更に、ステップS13において、インターフェース306を介して外部コンピュータ200よりデータA、B、C（日付、店番号、パスワード）を得る。

【0044】続いて、ステップS14において、暗号化部104が、データA～Eを用いて所定の演算処理（暗号化）を行い、チェックデータE<sub>N</sub>を発生する。ステップS15では、書込制御部105の制御により、ステップS13で獲得したデータA、B、Cと、ステップS14で獲得したチェックデータE<sub>N</sub>とを磁気ライタ103によって磁気ストライプ4に書込む。以上のようにして磁気ストライプ4にデータが書込まれたカードは、当該カード発行装置のカード排出部（不図示）より、排出され、識別カードとして発行される（ステップS16）。

【0045】なお、本実施形態では、光学的記録部分（ホログラムコードとバーコード）が記録された状態のカードを供給してカードの発行を行うものとするが、ホログラムコードの記録、バーコードの印刷をカード発行装置において行うようにしてもよい。この場合、データD及びデータEを発生し（或いはコンピュータ200より入力し）、これに従ってホログラムコード、バーコードの記録を行うことになる。なお、この場合、データD、データEは、記録に使用したデータを直接用いればよいので、カード発行装置100のホログラムリーダ101、バーコードリーダ302は不要となる。

【0046】図5は、本実施形態によるカード読取装置300の動作手順を説明するフローチャートである。カード読取装置300では、上述の手順で発行された識別カードの認証が行われる。

【0047】まず、ステップS21において、識別カード1のホログラムイメージに含まれるホログラムイメージ2をホログラムリーダ301で読み取り、これをデータD<sub>r</sub>（金額データ）とする。また、ステップS22において、識別カード1のバーコード3をバーコードリーダ302にて読み取り、これをデータE<sub>r</sub>（ID番号）とする。更に、磁気リーダ303によって磁気ストライプ4を読み取り、データA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>（日付、店番号、パスワード）を得る。更にステップS24では、磁気リーダ303が磁気ストライプ4よりチェックデータを読み取り、これをチェックデータE<sub>Nr</sub>とする。そして、ステップS25において、暗号化部304が上記ステップS21～23で得られたデータA<sub>r</sub>、B<sub>r</sub>、C<sub>r</sub>、D<sub>r</sub>、E<sub>r</sub>を用いて所定の演算処理（暗号化）を行い、チェックデータE<sub>Nr'</sub>を発生する。

【0048】ステップS26では、インターフェース305を介して、上記ステップS21～S23で獲得した

データA r～E rをコンピュータ200に送信し、コンピュータ200によってこれらのデータの正当性の検証を行う。なお、コンピュータ200による正当性の検証結果は、インターフェース305を介してカード読取装置300に入力される。ここで、データの正当性の検証としては、例えば日付が期限切れを示しているとか、店番号やパスワードが一致しない等が挙げられる。更に、カード発行装置100において読み取ったカードID番号（データE）をメモリ201に登録するように構成しておけば、カード番号の正、不正を判定することも可能である。もちろん、上述のように、カード毎にデータA、B、Cを異なる場合は、ID番号とデータA、B、Cを対応付けたテーブルを用いることになる。

【0049】ステップS27において、判定部3306は、コンピュータ200からの検証結果をチェックし、これが不正を示していた場合は、ステップS30において当該カードを拒否する。ここで、当該カードが不正である旨を表示するようにしてもよいことはいうまでもない。一方、コンピュータ200からの検証結果が正当であることを示していれば、処理はステップS27からS28へ進む。ステップS28では、磁気リーダ303で読み取ったチェックデータENrと、暗号化部304で算出したチェックデータENr'を比較し、両者が一致するか否かを調べる。両者が一致すれば、当該カードは正当であると判定され、ステップS29にてホログラムイメージ2に記録されていた金額データ（データDr）に従った金額が支払われる。一方、両者が一致しなければ、当該カードは不正であるとして、ステップS30へ進み、当該カードを拒否する。

【0050】なお、上記ステップS11～ステップS13、或いはステップS21～S24における各データの獲得は、これらフローチャートによって示された順番に限られるものではないし、実質的に同時に獲得されてもよい。

【0051】また、上記実施形態では、カード読取装置300がコンピュータ200と通信することにより、データA r、B r、C r等の正当性を検証するが、この構成は省略してもよい。即ち、図3に示したカード読取装置300の構成のうちインターフェース305を省略し、図5のフローチャートからステップS26、S27を省略してもよい。この場合、磁気ストライプから得たチェックデータENrと暗号化部304で発生したチェックデータENr'との一致を調べることのみで識別カードの正当性を判定することになるが、ホログラムコードとして記録されているデータDによって、磁気ストライプ4に書込むべきチェックデータが変化するので、識別カードのセキュリティを効果的に向上することができる。

【0052】なお、上記実施形態のカード読取装置において、使用済みとなったカードの磁気ストライプ4上に

記録されたデータを消去あるいは無効化する構成を備えてもよい。

【0053】次に、上記実施形態におけるセキュリティ向上システムの変形例を図6、図7を参照して説明する。

【0054】図6は、本実施形態のセキュリティ向上システムにおける第1の変形例によるカード読取装置の構成を示す図である。なお、図6において図2と同じ構成には同一の参照番号を付し、ここでは説明を省略する。第1の変形例では、データA、B、Cを磁気ストライプ4に書き込まない。即ち、図4のステップS15において、図2の書込制御装置105は磁気ライタ103を用いて暗号化部104より入力したチェックデータENのみを磁気ストライプ4に書き込むことになる。

【0055】さて、図6においてインターフェース310は、コンピュータ200よりデータA、B、Cを受信し、これを暗号化部304へ出力する。暗号化部304は入力されたA、B、C、Dr、Erに基づいてチェックデータENr'を生成する。そして、判定部311は、暗号化部304より得たチェックデータENr'と磁気リーダ303が磁気ストライプ4を読み取って得たチェックデータENrとを比較し、両者が一致するか否かでカードの正当性を判定する。

【0056】図7は第1の変形例におけるカード読取装置350の制御手順を示すフローチャートである。同図において、図5と同じ処理を行うステップには同一のステップ番号を付し、ここでは詳細な説明を省略する。ステップS41では、インターフェース310を介して外部コンピュータ200よりデータA、B、Cを獲得する。そして、ステップS42では、獲得したデータA、B、C、Dr、Erに基づいて暗号化部304がチェックデータENr'を算出する。そして、このチェックデータENr'とステップS24で獲得したチェックデータENrとを比較してカードの正当性が判定される。

【0057】なお、上記第1の変形例では、磁気ストライプ4にチェックデータENを記録し、データA、B、Cの記録は行わなかったが、データA～Cとチェックデータの保存先としては更に種々の変形が可能である。例えば、チェックデータENとデータAを磁気ストライプ4に記録するようにしてもよい。また、チェックデータENの書込先をメモリ201としてもよい。以下、第2の変形例として、チェックデータENの書込先をメモリ201とし、磁気ストライプ4には何も記録しない場合を説明する。

【0058】図8は本実施形態のセキュリティ向上システムにおける第2の変形例によるカード読取装置の構成を示すブロック図である。第2の変形例では、図2のカード発行装置100において、書込制御部105は、磁気ストライプ4へのチェックデータENの書き込みを行わないほか、他のデータA～Cの書き込みも行わないもの

とする。従って、識別カード1において磁気ストライプ4を省略することも可能である。そのかわりに、書込制御装置105は、コンピュータ200に対してチェックデータEN、データD（金額データ）、データE（ID番号）を送出するものとする。

【0059】カード発行装置よりチェックデータEN、データD、データEを受け取ったコンピュータ200は、データD、データEにチェックデータENを対応付けたチェックデータテーブル202（図8参照）を生成してメモリ201に記録する。なお、データEが各識別カードに固有の番号を有するので、データEのみを用いてチェックデータを登録するようにしてもよい。この場合、チェックデータテーブル202は、データEとチェックデータENのみを対応付けたテーブルとなる。要するに、カード読取装置360において識別カード1'のホログラムイメージ2もしくはバーコード3を読み取って得られたデータに基づいて、チェックデータテーブル202中のチェックデータを唯一特定できればよいのである。

【0060】図8に示された識別カード1'には磁気ストライプが省略されており、カード読取装置360においては磁気リーダが省略されている。

【0061】上述の第1の変形例と同様に、暗号化部304はインターフェース320を介してコンピュータ200より入力したデータA、B、Cと、ホログラムリーダ301より入力したデータDr及びバーコードリーダ302より入力したデータErを用いてチェックデータENr'を算出する。この算出されたチェックデータENr'は判定部311へ入力される。

【0062】一方、インターフェース320は、ホログラムリーダ301より得られたデータDr及びバーコードリーダ302より得られたデータErをコンピュータ200へ出力する。コンピュータ200は、カード読取装置360より入力されたデータDr及びデータErを用いてチェックデータテーブル202を検索し、対応するチェックデータENを出力する。コンピュータ200より出力されたチェックデータENはインターフェース320を介して判定部311へ入力される。

【0063】判定部311は暗号化部304より入力されたチェックデータENr'をインターフェース320を介して入力されたチェックデータENとを比較することにより当該識別カード1'の正当性を判定する。なお、第2の変形例におけるカード読取装置によるカードの正当性チェックの制御は、上述の図7とほぼ同様である。ただし、ステップS24においてチェックデータEN（図6のENrに相当する）を獲得するに際して、データEr、データDrをコンピュータ200に送り、その応答としてチェックデータENを獲得する点が異なる。

【0064】以上説明したように、上記実施形態のカ

ドセキュリティ向上システムによれば、カード発行時に外部より与えられたデータA～C（実施形態ではコンピュータ200より入力される）を用いてチェックデータの処理が行われる。従って、例えばデータA～Cを定期的に変更することでシステムのセキュリティを更に向上することが可能である。更に、チェックデータ算出のためにホログラムイメージ2が用いられるので、システムのセキュリティが向上する。

【0065】なお、上記実施形態におけるデータの種類とその記録方法は一例にすぎず、種々の変更が可能であることはいうまでもない。たとえば、識別カードのID番号をホログラムコードとして登録するようにしてもよい。

【0066】また、上記実施形態においてチェックデータ等を識別カード1に書き込む場合の書込先を磁気ストライプとしたが、ホログラムやバーコード等の光学的読取記録部分に記録するようにしてもよい。更に識別カードにICメモリを搭載しておき、これに種々のデータを記録することも可能である。また、光学的読取部分や磁気的読取部分もカード上に複数個存在してよいことはいうまでもない。

【0067】更に、上記実施形態では、コンピュータ200をカード発行装置及びカード読取装置のいずれからも独立したものとしたが、コンピュータ200はカード発行装置もしくはカード読取装置の何れか一方に内蔵されてもよい。また、この場合、カード発行装置、カード読取装置の何れかのCPUがコンピュータ200の機能を兼ね備えるものとしてもよい。

【0068】また、上記実施形態のカードセキュリティシステムは、ホログラムイメージにホログラムイメージ2を含ませたことで、そのセキュリティをよりいっそう向上している。以下、本実施形態によるホログラムコードを記録したホログラムカードと、当該ホログラムコードを読みとるホログラムリーダの詳細な構成について説明する。

【0069】ホログラムは、ホログラフィック手法あるいはダイレクトパターンイメージング手法を用いて記録される。ホログラムは、フーリエ変換型ホログラムであってもよいし、フレネル型ホログラムであってもよい。

【0070】ここでは、フーリエ変換ホログラムを採用し、そのイメージパターンはバーコード像とする。更に、ホログラムのイメージパターンとしては、ランダムパターン、モアレパターン、逆フーリエ変換パターン等のいずれであってもよいし、これらの組み合わせであってもよい。図9はバーコード状パターンの一例を示す図である。以下では、このようなバーコード状パターンを再生するフーリエ変換パターンを記録する場合のホログラム記録と読み取りを説明する。

【0071】図10A及び図10Bは、フーリエ変換パターンのホログラム記録及び再生方法を説明する図であ

る。図10Aは典型的なホログラム記録の構成を示している。所定のパターン（本例では図9の如きバーコード状パターン）51より距離f（fはフーリエ変換レンズ52の前方焦点距離）だけ離れた位置にフーリエ変換レンズ52がセットされる。なお、パターン51には、必要に応じて散光器が結合される。記録媒体53は、フーリエ変換レンズ52の後方に、当該レンズ52の後方焦点距離（=f）だけ離れた位置に配置される。光源光54をパターン51に図示のように照射するとともに、参照光55を記録媒体上へ所定角度θで照射する。すると、フーリエ変換レンズ52を介して記録媒体53へ到達するパターン光と参照光54が記録媒体53の面上で干渉し、パターン51に対応するフーリエ変換ホログラムパターンが記録媒体53の全体あるいは一部分に形成され、記録される。

【0072】図10Bには、フーリエ変換ホログラムにおける画像の再生方法が示されている。参照光55の共役光としてのコリメート光56を、当該ホログラムをエンコードした工程における参照光の照射角度θで、図示のように記録媒体53に照射する。すると、フーリエ変換レンズ57を介して、その前方焦点距離上に実像58が再生される。なお、上記説明では、ホログラムの記録時にフーリエ変換レンズを用いたが、いわゆるレンズ無しフーリエ変換ホログラム記録の手法を用いることも可能である。

【0073】上述のようなフーリエ変換記録手法は、高いセキュリティを提供する。なぜならば、ホログラム記録時の光学的仕様として、参照光の角度のみならず、その波長やフーリエ変換レンズの特性を知らない限り、当該ホログラムイメージを認識することが極めて困難だからである。

【0074】図11は、本実施形態によるカード読取装置のホログラムリーダの詳細な構成を説明する図である。

【0075】71は識別カード1上に形成されたホログラムイメージである。72はホログラムを照射するための光源である。73は、光源72より照射された光によって再生された再生像である。なお、フーリエ変換ホログラムの場合は、ホログラムイメージ71と再生像73との間の適切な位置にフーリエ変換レンズ57（図10B参照）が配置されるが、図示を省略してある。ただし、ホログラムがいわゆるフレンネル型ホログラムであれば、そのような変換レンズは不要である。

【0076】74は光学的処理部であり、再生像73を光学的に処理し、所定のパターン75（本例ではバーコード状パターンであり、以下バーコードパターン75という））を形成し、出力する。76は光センサーであり、バーコードパターン75を走査して、光強度に応じた信号を出力する。

【0077】なお、本実施形態のホログラムリーダは、

ホログラムイメージから最終的に図9のようなバーコード像を再生する。しかしながら、本実施形態のホログラムイメージは、当該バーコード像に所定のパターンを干渉させたイメージが記録されている。従って、フーリエ変換型ホログラム手法で記録されたホログラムイメージに適切な光源72よりの光を照射することにより、不図示のフーリエ変換レンズを経て再生像73が空間に検出され得るが、この再生像73自体ではなんの意味もない。しかし、これが光学的処理部74によって処理されると、バーコードパターン75として空間に再生されるのである。

【0078】図12は光学的処理部74の構成を示すブロック図である。同図において、再生像73に対応する再生光はビームスプリッタ741を通過して、ミラー742で反射される。ミラー742による反射光はビームスプリッタ741で反射されて、90度方向を換える。一方、干渉用入力パターンに対応する光がビームスプリッタ741を通過する。この結果、ミラー742で反射された再生光と干渉用入力パターン743に対応するパターン光とが干渉し、新たなパターン像が生成される。この新たなパターン像がバーコードパターン75であり、読み取可能なパターンとして光センサー76に提供される。

【0079】以上のように光学的処理部74によって再生されたバーコードパターン75は、光センサー76によって検出される。光センサー76は、バーコードパターン75の光強度分布に応じた信号を信号処理部79に出力する。信号処理部79は、光センサー76より入力された信号を2値データを示す矩形状のパルス列に変換する。ここで、2値化は、当該バーコードパターン75の相対的な光強度分布に基づいてなされる。例えば、2値化のための閾値を、光センサーの最大レベル（バーコードパターンの白部分）と最低レベル（バーコードパターンの黒部分）との値に基づいて決定する（たとえば両者の平均値）ようにすれば、より良好かつ確実にバーコードパターンを認識することができる。

【0080】以上のように、ホログラムとして記録するパターンに、巧みに設計されたランダムパターンを用いれば、フーリエ変換面においてさえも、何の意味をも有していないパターンとしか認識されない。この場合、もう一つの別のパターンを用意しておき、再生されたランダムパターンを有意味なパターンに変換し、これを光センサー76によって検出するようにする。ここで、ランダムパターンを有意味なパターンに変換するのが、光学的処理部74である。そして、光センサー76は、この有意味なパターンの光強度を検出し、信号処理部79がこれの検出結果に基づいて2値データを発生する。たとえば、ホログラムイメージとしての記録にモアレパターンを用いた場合は、別のモアレパターンに干渉することで、予め設計されたバーコードパターンを得ることがで

きる。

【0081】なお、再生されたバーコードパターン75の光センサ76による走査は、光センサ76がバーコードパターンを走査するような構成としてもよいし、光センサ76は1点の光強度を検出し、読み取り時に識別カード1を移動させることによって再生像であるバーコードパターン75を移動させ、この移動によってバーコードパターンを走査するようにしてもよい。

【0082】また、再生像であるバーコードパターン75の白黒パターンの強弱の度合は、カード表面の部分的な損傷や歪み等のためにオリジナルの記録イメージとは若干異なる可能性がある。しかしながら、光センサ76及び信号処理部79は、上述のごとく、光の相対的な強度を調べ、2値データとして出力するので、このような障害があってもバーコードパターンを正しく読み取ることができる。

【0083】なお、光学的処理部74は、ランダムパターンやモアレパターン、逆フーリエ変換パターンが記録されたホログラムコードを読み取る場合に必要な構成である。しかしながら、再生像がそのまま有意味なバーコードパターンとなる場合には、光学的処理部74は不要である。図13は光学的処理部を省略したホログラムリーダの構成を示す図である。光源72よりの光をホログラムイメージ（ホログラムコード）に照射することで、空間にバーコードイメージ77が再生されるので、光センサ76によってその光の強度を直接的に読み取ることができる。なお、フーリエ変換形ホログラムの場合は、図13の再生像77とホログラム71との間にフーリエ変換レンズが存在していることはいうまでもない。

【0084】また、光学的処理部74の機能をデジタル的に実現することも可能である。この場合、図11の構成において、再生像73の光強度分布を直接光センサ76によって検出し、これをデジタルデータとして信号処理部79に送る。信号処理部79では、数値演算によって図12の干渉用入力パターン743を干渉させたのと等価の処理を行う。この数値演算の結果得られる光強度分布のデジタルデータは、バーコードパターン75に対応したものとなる。

【0085】更に、光学的処理部74は光波面の干渉を利用したものであってもよい。例えば球面波と平面波を干渉させると円形状の縞パターンが得られ、平面波と平面波を干渉させると、バーコード状の縞パターンが得られる。従って、例えば、ホログラムイメージからの再生光として球面波が得られるように構成し、光学的処理部74において干渉用入力パターンとして平面波を入力すれば、バーコードパターン75が得られるようになり、光センサで読み取ることができる。このようにホログラムからの反射光の位相分布によって情報を検出することも可能である。

【0086】以上説明したように、上記実施形態によれ

ば、特殊なデータチェックシステムを用いている上に、特殊なホログラムとホログラム検出方法を用いているのでカードセキュリティが飛躍的に向上する。更に再生されたホログラムパターンの認識を、パターンの相対的な光強度をチェックするということで行うので、カードの部分的な損傷等があっても、正しく認識を行うことができる。

【0087】また、ホログラムイメージとして、他の所定パターンを干渉させることで初めて意味のある再生像を得られるよう構成したので、セキュリティがいちじるしく向上する。

【0088】なお、上記信号処理部79における2値データ（矩形信号）への変換は、バーコード等の技術において周知のセルフクロッキング（self-clocking）の方法に基づいて行われるものとする。また、識別カード表面の近くの空間へのイメージの再生は、一般の照明光では見ることができず、適した光学系（たとえば、ホログラムイメージへの光の照射角、照射光の波長、ホログラム記録時のフーリエ変換レンズに対応した適切な特性を有するフーリエ逆変換レンズ）によってのみ再生され、光センサ76によって読み取ることが可能となる。このため、セキュリティが向上する。

【0089】

【発明の効果】以上説明したように、本発明によれば、カード等のセキュリティが効果的に、かつ飛躍的に向上する。

【0090】

【図面の簡単な説明】

【図1】本実施形態のカードセキュリティシステムに用いられる識別カードの概観を示す図である。

【図2】本実施形態のカードセキュリティシステムにおけるカード発行装置の構成を示すブロック図である。

【図3】本実施形態におけるカード読取装置の構成を示すブロック図である。

【図4】第1の実施形態によるカード発行装置100の動作手順を説明するフローチャートである。

【図5】本実施形態によるカード読取装置300の動作手順を説明するフローチャートである。

【図6】本実施形態のセキュリティ向上システムにおける第1の変形例によるカード読取装置の構成を示す図である。

【図7】第1の変形例におけるカード読取装置350の制御手順を示すフローチャートである。

【図8】本実施形態のセキュリティ向上システムにおける第2の変形例によるカード読取装置の構成を示すブロック図である。

【図9】バーコード状パターンの一例を示す図である。

【図10A】フーリエ変換パターンのホログラム記録方法を説明する図である。

【図10B】フーリエ変換パターンのホログラム再生方

法を説明する図である。

【図1 1】本実施形態によるカード読取装置のホログラムリーダの詳細な構成を説明する図である。

【図1 2】光学的処理部74の構成を示すブロック図である。

【図1 3】光学的処理部を省略したホログラムリーダの構成を示す図である。

【符号の簡単な説明】

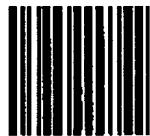
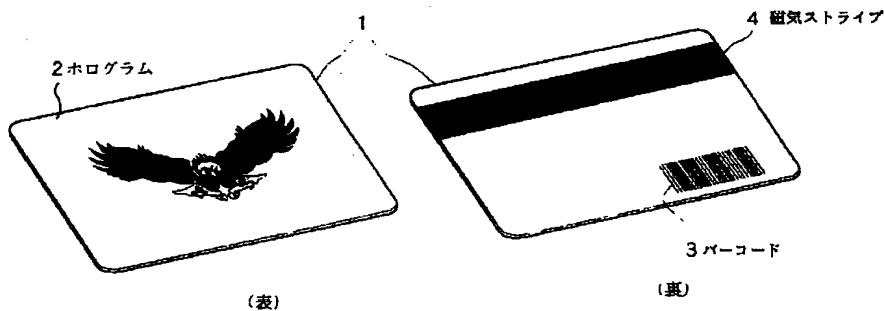
- 1 識別カード
- 2 ホログラムイメージ
- 3 バーコード

#### 4 磁気ストライプ

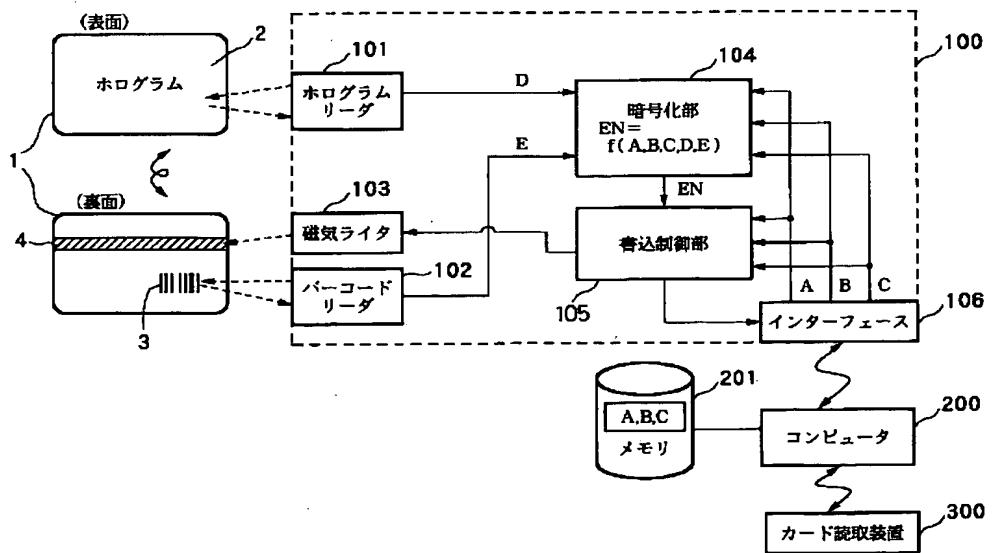
- 100 カード発行装置
- 101 ホログラムリーダ
- 102 バーコードリーダ
- 103 磁気ライタ
- 104 暗号化部
- 105 書込制御部
- 106 インターフェース
- 200 コンピュータ
- 201 メモリ
- 300 カード読取装置

【図1】

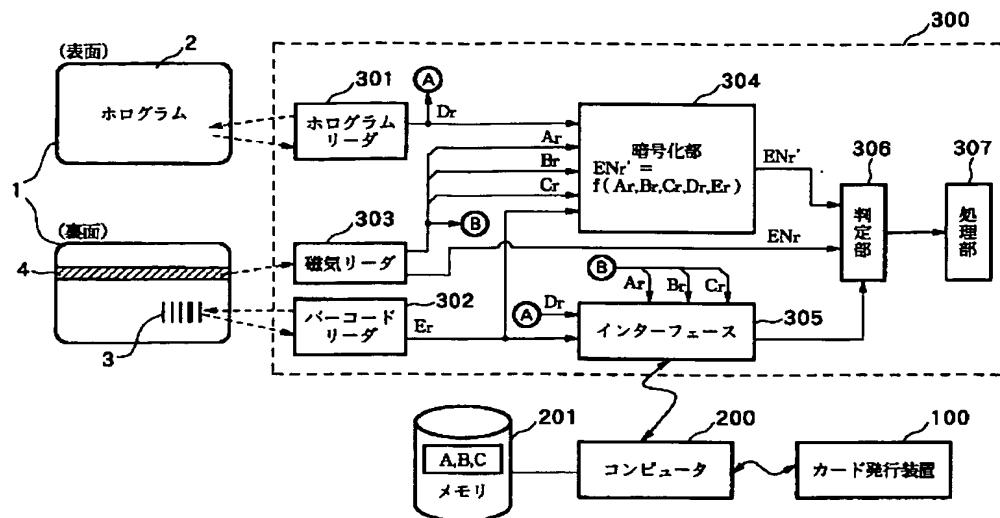
【図9】



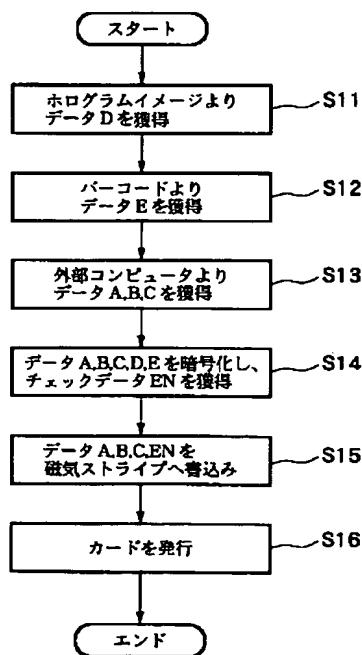
【図2】



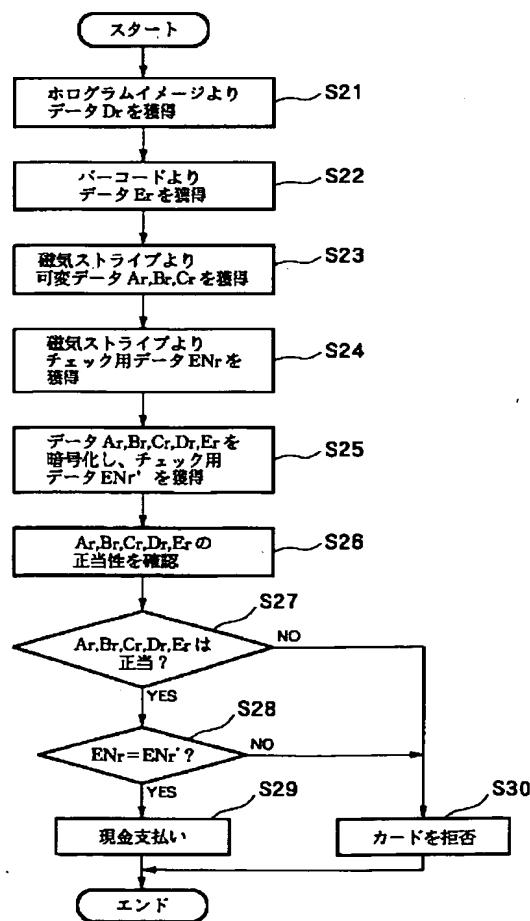
【図3】



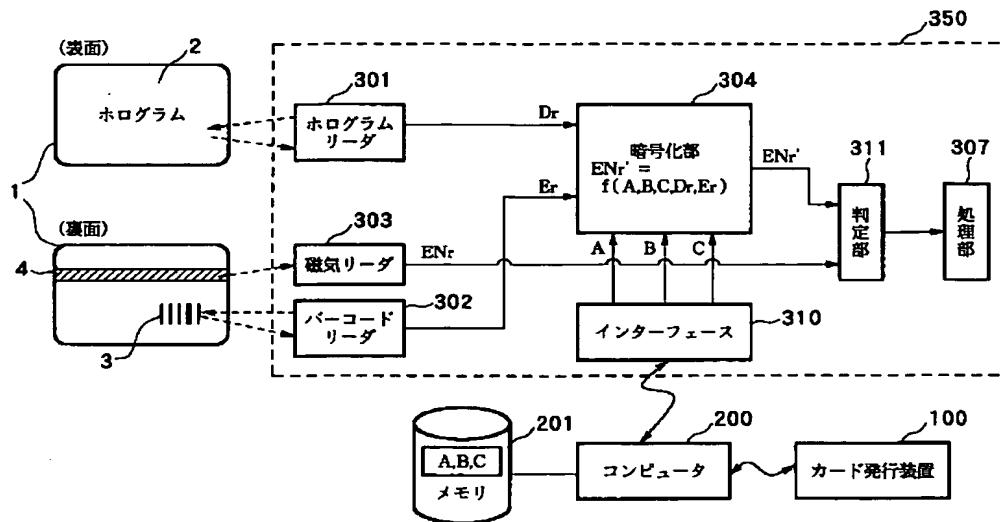
【図4】



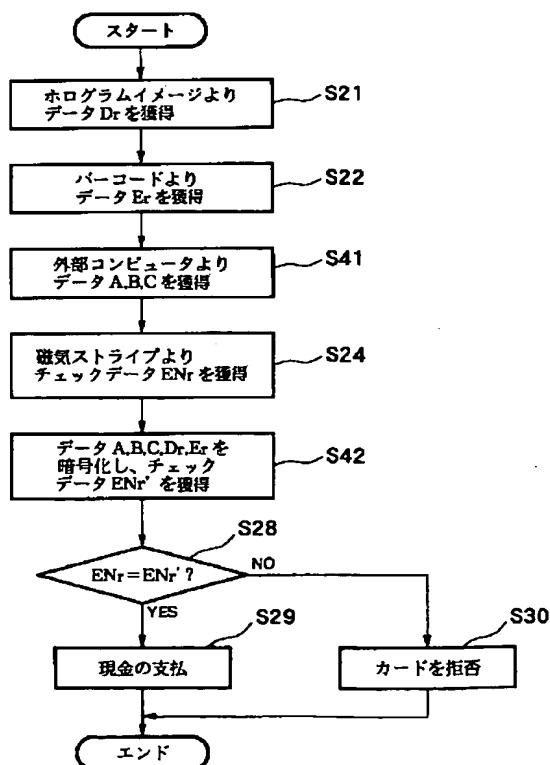
【図5】



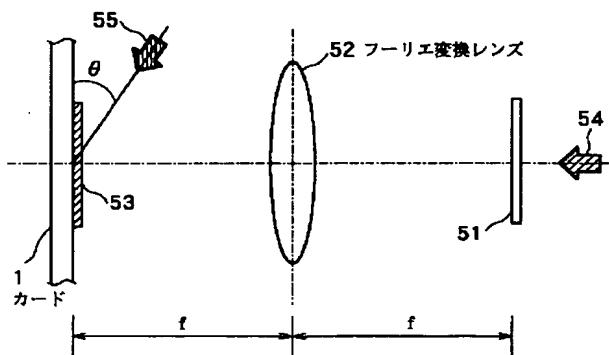
【図6】



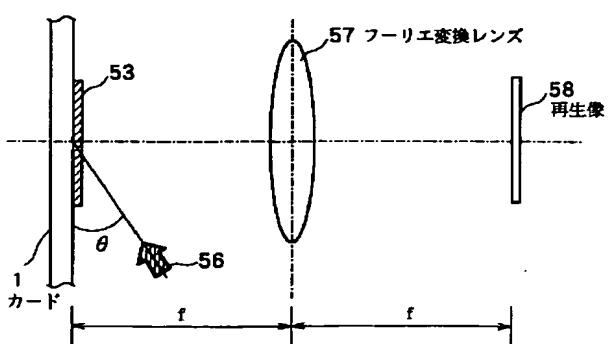
〔図7〕



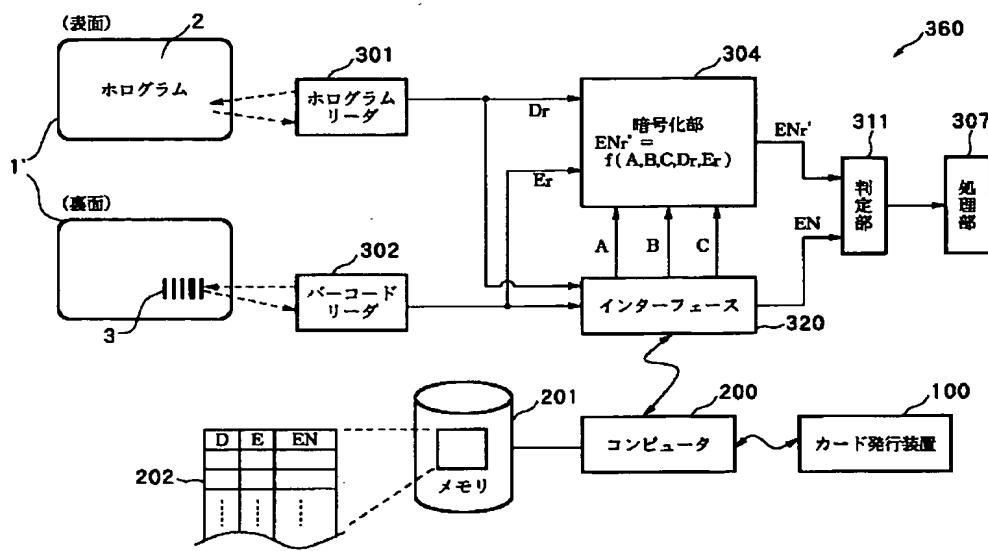
### 【図10A】



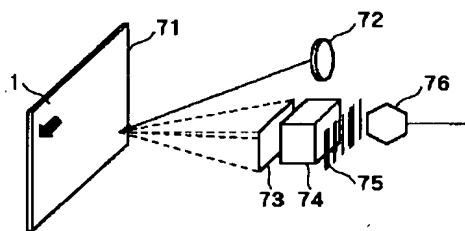
【図10B】



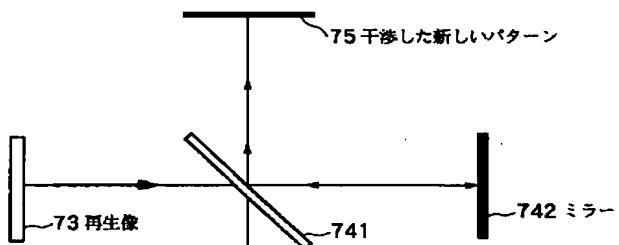
【図8】



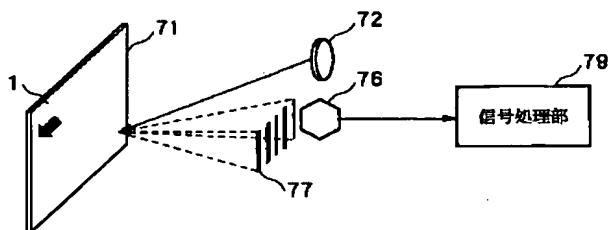
【図11】



【図12】



【図13】



75 干渉した新しいパターン

73 再生像

742 ミラー

743 干渉、比較用入力パターン

フロントページの続き

(51) Int.Cl. 6  
G 0 6 K 19/06

識別記号

F I  
G 0 6 K 19/00

D

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**